**Amendments to the Specification:**

Please replace the paragraph beginning on page 1, line 5 with the following rewritten paragraph:

This application claims priority from U.S. Provisional Application No. 60/197,152, entitled CRYPTOGRAPHY PROCESSING UNIT, filed April 13, 2000; and claims priority from U.S. Provisional Application No. 60/261,425, entitled UBIQUITOUS BROADBAND SECURITY CHIP, filed January 12, 2001, the disclosures of which are herein incorporated by reference herein ~~for all purposes~~.

Please replace the paragraph beginning on page 6, line 1 with the following rewritten paragraph:

In general, the present invention provides an architecture (hardware implementation) for an authentication engine to increase the speed at which multi-loop and/or multi-round authentication algorithms may be performed on data packets transmitted over a computer network. As described in this application, the invention has particular application to the variants of the SHA1 and MD5 authentication algorithms specified by the IPSec cryptography standard. In accordance with the IPSec standard, the invention may be used in conjunction with data ~~encryption/encryption~~ encryption/decryption architecture and protocols. However it is also suitable for use in

conjunction with other non-IPSec cryptography algorithms, and for applications in which encryption/decryption is not conducted (in IPSec or not) and where it is purely authentication that is accelerated. Among other advantages, an authentication engine in accordance with the present invention provides improved performance with regard to the processing of short data packets.

Please replace the paragraph beginning on page 6, line 14 with the following rewritten paragraph:

Authentication engines in accordance with the present invention apply a variety of techniques that may include, in various applications, collapsing two-multi-round authentication algorithm (e.g., SHA1 or MD5 or variants) processing rounds into one; reducing operational overhead by scheduling the additions required by a multi-round authentication algorithm in such a ~~matter~~ manner as to reduce the overall critical timing path ("hiding the adds"); and, for a multi-loop (e.g., HMAC) variant of a multi-round authentication algorithm, pipelining the inner and outer loops. In one particular example of applying the invention in an authentication engine using the HMAC-SHA1 algorithm of the IPSec protocol, collapsing of the conventional 80 SHA1 rounds into 40 rounds, hiding the adds, and pipelining the inner and outer loops allows HMAC-SHA1 to be conducted in approximately the same time as conventional SHA1.

Please replace the paragraph beginning on page 11, line 14 with the following rewritten paragraph:

In general, the present invention provides an architecture (hardware implementation) for an authentication engine to increase the speed at which multi-loop and/or multi-round authentication algorithms may be performed on data packets transmitted over a computer network. Authentication engines in accordance with the present invention apply a variety of techniques that may include, in various applications, collapsing two multi-round authentication algorithm (e.g. SHA1 or MD5 or variants) processing rounds into one; reducing operational overhead by scheduling the additions required by a multi-round authentication algorithm (e.g., SHA1 or variants) in such a ~~matter~~ manner as to reduce the overall critical timing path ("hiding the adds"); and, for an HMAC (multi loop) variant of a multi-round authentication algorithm, pipelining the inner and outer loops. Among other advantages, an authentication engine in accordance with the present invention provides improved performance with regard to the processing of short data packets.

Please replace the paragraph beginning on page 14, line 20 with the following rewritten paragraph:

The engine 200, further includes a dual-ported ROM 218. The dual-ported ROM 218 further facilitates the parallel inner and outer ~~has~~ hash operations by allowing for concurrent constant lookups both by inner and outer hash engines.